

### Mathematical Transition

For the construction of the regular pentagon, we used the five solutions,  $z_0, z_1, z_2, z_3, z_4$ , of

$$Z^5 - 1 = 0,$$

thus the five numbers

$$z_k = \cos(2\pi k/5) + i \sin(2\pi k/5), \quad k = 0, 1, 2, 3, 4.$$

The first of these is just 1 and was of little interest. All the others were from an *algebraic* point of view equivalent and all satisfied the equation

$$Z^4 + Z^3 + Z^2 + Z + 1 = 0.$$

We could have singled out  $\cos(2\pi/5) + i \sin(2\pi/5)$  as being from a *geometrical* point of view the obvious choice.

For the construction of the regular heptadecagon, we used the sixteen solutions,  $z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8, z_9, z_{10}, z_{11}, z_{12}, z_{13}, z_{14}, z_{15}, z_{16}$ , of

$$Z^{16} + Z^{15} + Z^{14} + \dots + Z^1 + 1 = 0.$$

They are

$$Z_k = \cos(2\pi k/17) + i \sin(2\pi k/17).$$

In both cases, it was the symmetries that were of principal interest and what we studied was the effect of these symmetries not alone on  $z_1, z_2, \dots$  but on all the numbers

$$a_1 z_1 + a_2 z_2 + a_3 z_3 + \dots,$$

where  $a_1, a_2, a_3, \dots$  were arbitrary rational numbers, thus fractions.

If we had studied the equilateral triangle, which we left aside as too simple, we would have used the three numbers

$$z_k = \cos(2\pi k/3) + i \sin(2\pi k/3), k = 0, 1, 2,$$

of which now only two are of much algebraic interest, namely

$$z_1 = \cos(2\pi/3) + i \sin(2\pi/3), \quad z_2 = \cos(4\pi/3) + i \sin(4\pi/3).$$

Both satisfy the equation

$$Z^2 + Z + 1 = 0,$$

which can be solved to yield

$$\frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$$

Comparing signs, we see that

$$z_1 = \frac{-1 + i\sqrt{3}}{2}$$

This is the number that I now call simply  $\alpha$ . This is partly because, as often happens, I have simply taken over a notation from others, but also because we are interested in quite different properties of the numbers

$$a_1 z_1 + a_2 z_2$$

or, more generally, if we were studying Fermat's equation for  $n = 5$ ,  $n = 17$  or any other prime of the numbers

$$a_1 z_1 + a_2 z_2 + \dots + a_{n-2} z_{n-2} + a_{n-1} z_{n-1},$$

where, for example,  $n - 1$  is 4 if  $n = 5$  or 16 if  $n = 17$ .

For the moment, since these properties are rather difficult, we confine ourselves to  $n = 3$ . Then

$$a_1 z_1 + a_2 z_2 = a_1 \alpha + a_2 \alpha^2 = a_1 \alpha - a_2(1 + \alpha) = a + b\alpha,$$

with  $a = -a_2$ ,  $b = a_1 - a_2$ .

In the earlier approaches to Fermat's theorem, for  $n = 3$  in particular, what is important are primes: ordinary primes in Euler's treatment and primes in a more exotic setting for a treatment modelled on Kummer's general methods. Primes are integers. So we need to use only integral numbers of the form  $a + b\alpha$ . We can naively expect that such a number will be integral if  $a$  and  $b$  are not merely rational numbers but in fact whole numbers, that is integers. The naive expectation is borne out by experience. I even give the domain of such numbers a special symbol  $\mathbb{Z}(\alpha)$ . The domain for  $n = 3$  is much simpler than it will be for  $n > 3$ .

Any complex number is represented in the plane. This is true not only of  $\alpha$  but of all the numbers  $a + b\alpha$ . The norm of a complex number  $z = x + iy$  is *for us* the *square* of its distance from the origin. Thus the norm of  $1 + i$  is 2, that of  $2 + 7i$  is  $4 + 49 = 53$ . This norm is

$$z\bar{z} = (x + yi) \times (x - yi) = x^2 + y^2.$$

Thus the norm of  $\alpha$  is

$$\cos^2(2\pi/3) + \sin^2(2\pi/3) = \frac{1}{4} + \frac{3}{4} = 1,$$

and so is that of  $\alpha^2 = -1 - \alpha = \bar{\alpha}$ ,

$$\alpha^2 = \frac{-1 - i\sqrt{3}}{2}.$$

## More about norms.

We have stressed that  $z \rightarrow \bar{z}$  is a symmetry of the collection of complex numbers, which arises because  $i$  and  $-i$  are both algebraic symbols with exactly the same properties. The distinction between the two only arises in the geometric representation. The point representing  $i$  lies above the axis of abscissas and the point representing  $-i$  lies below it. Since it is a symmetry – as is readily verified – it must respect multiplication

$$\bar{w} \times \bar{z} = z \times w.$$

Thus

$$N(z \cdot w) = (z \cdot w) \cdot (z \cdot w) = z \cdot w \cdot \bar{z} \cdot \bar{w} = z\bar{z} \cdot w\bar{w} = N z \cdot N w.$$

This formal property appears for other definitions of norms, norms that have no relation to length. Consider, for example, a new domain, the domain of numbers  $c + d\sqrt{3}$ , where  $c$  and  $d$  are now integers. It is different from  $Z(\alpha)$  because

$$a + b\alpha = \left(a - \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3} = c + d\sqrt{-3}.$$

Not only is  $-3$  replaced by  $3$ , the important point, but in the new domain the coefficients  $c$  and  $d$  are to be whole numbers, whereas in  $Z(\alpha)$ , they may be half-integers. The second point is too subtle for us to linger on it here. It arises because

$$N\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right) = \frac{1}{4} + \frac{3}{4} = 1$$

is integral.

On the other hand in the new domain there is also a symmetry. It sends  $\sqrt{3}$  to  $-\sqrt{3}$  and thus

$$c + d\sqrt{3} \rightarrow c - d\sqrt{3}.$$

Since  $\sqrt{3}$  and  $-\sqrt{3}$  satisfy exactly the same equation with rational coefficients, namely

$$Z^2 - 3 = 0,$$

they are indistinguishable if one's only reference points are rational numbers. That is what permits the symmetry.

Thus

$$(a+b\sqrt{3})(c+d\sqrt{3})=(ac+3bd)+(ad+bc)\sqrt{3}\rightarrow(ac+3bd)-(ad+bc)\sqrt{3}=(a-b\sqrt{3})(c-d\sqrt{3})$$

and

$$(a+b\sqrt{3})+(c+d\sqrt{3})=(a+c)+(b+d\sqrt{3})\rightarrow(a+c)-(b+d)\sqrt{3}=(a-b\sqrt{3})+(c-d\sqrt{3})$$

This new and different norm was the norm that we used to study the identity

$$(A) \quad 2 = \sqrt[3]{6\sqrt{3} + 10} - \sqrt[3]{6\sqrt{3} - 10}.$$

We noted that

$$N(6\sqrt{3} + 10) = 100 - 3 \cdot 36 = -8$$

and that  $-8$  was a cube.

The numbers in the new domain are all real and the norm is no longer a distance. It is just a convenient algebraic device. If we want to think of  $\sqrt{3}$  as an ordinary real number then it is approximately 1.73205. Thus  $1 + \sqrt{3}$  is approximately 2.73205 and  $1 - \sqrt{3}$  is approximately  $-.73205$  but their product, which is the norm of either is  $-2$ . Another example is  $17 - 10\sqrt{3}$  which under the symmetry becomes  $17 + 10\sqrt{3}$ . Their norm is

$$(17 - 10\sqrt{3})(17 + 10\sqrt{3}) = 289 - 300 = -11.$$

These numbers are as decimals approximately  $-.320508$  and  $34.3205$ , but in algebraic investigations their decimal expansion should be studiously ignored. It is irrelevant!

The identity (A) is valid. The question is whether it is remarkable. It certainly appears strange. My point was that it is striking not because it expresses any profound or even curious mathematical truth, but only because our unfamiliarity with numbers formed from surds prevents our recognizing easily that both the numbers under the cube-root signs are cubes. Once we do so, we see that the identity becomes

$$\sqrt[3]{(1 + \sqrt{3})^3} + \sqrt[3]{(1 - \sqrt{3})^3} = 2,$$

and no-one would claim that this is remarkable. It is trivial!

## Afterthought

The remarkable formula is a consequence of a general formula, the formula of Del Ferro, for the solution of a cubic equation.

$$\begin{aligned}X^3 + PX &= Q \\ \Delta &= \frac{Q^2}{4} + \frac{P^3}{27} \\ X &= \sqrt[3]{\sqrt{\Delta} + \frac{Q}{2}} - \sqrt[3]{\sqrt{\Delta} - \frac{Q}{2}}\end{aligned}$$

This is of course, as Varadarajan remarks, a very beautiful formula, even today. Applied to

$$X^3 + 6X = 20,$$

which has the root 2, it yields the initial identity

$$(A) \quad \sqrt[3]{6\sqrt{3} + 10} - \sqrt[3]{6\sqrt{3} - 10}.$$

Del Ferro's dates are 1465-1526, thus long before Kummer and Galois. In the fifteenth or sixteenth century, recognizing that a number formed from the square root of 3 was a cube was an altogether different matter than it is today. So, if the formula was regarded as remarkable then, it was with good reason. Once again, I have to admit that I am unfamiliar with the response to such formulas at the time of their discovery and subsequently.

On the other hand, I began by observing that it is only familiarity with the ideas of Kummer and Galois that made me suspicious, and the reason for introducing the example is not to suggest that someone unfamiliar with what might be called higher mathematics or modern algebra has no right to be astonished, but rather to emphasize that calculations within domains such as  $\mathbb{Z}(\alpha)$  or

$$\mathbb{Z}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$$

are not easily made and require practice and experience. We are trying to acquire them.

When we come to Kummer, we shall see that he replaces the solution  $\alpha = \cos(2\pi/3) + i \sin(2\pi/3)$  of

$$Z^2 + Z + 1 = 0$$

by the solution  $\alpha = \cos(2\pi/n) + i \sin(2\pi/n)$  of

$$Z^{n-1} + Z^{n-2} + Z^{n-3} + \dots + Z^2 + Z + 1 = 0,$$

The number  $n$  becoming an arbitrary odd prime.

$$n = 3, 5, 7, 11, 13, 17, 19, 23, 31, \dots,$$

23 being particularly fateful. The domain  $\mathbb{Z}(\alpha)$  is different in each case.

There are two difficulties that appear, one immediately for  $n = 5$ . The first is that there are no longer just a finite number of units to cause trouble. For  $n > 3$ , there are an infinite number. The second is that from 23 on there is no longer unique factorization. Thus before we see how Kummer was able to overcome these problems, we had best understand in the simplest case,  $n = 3$ , what difficulties the units cause and what advantages unique factorization possesses, even indeed what unique factorization is. How can it be exploited to prove Fermat's theorem for  $n = 3$ ? We will then be in a better position to appreciate Kummer's achievement in doing without it. Euclid's discussion of primes and of the greatest common measure of two numbers is perhaps of considerable historical interest, but, I now see, hardly the right introduction to an adequate understanding of the modern notion.

## SOME NAMES AND DATES

Carl Friedrich Gauß (1777-1855).

Gabriel Lamé (1795-1870).

Niels Henrik Abel (1802-1829).

Carl Gustav Jacob Jacobi (1804-1851).

Peter Gustav Lejeune Dirichlet (1805-1859).

Ernst Eduard Kummer (1810-1893).

Leopold Kronecker (1823-1891).

Gotthold Eisenstein (1823-1852).

Richard Dedekind (1831-1916).

*Disquisitiones Arithmeticae* 1801



## SOME BACKGROUND READING

Two articles by H. M. Edwards in the *Archive for the History of Exact Sciences*.

*The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes*, vol. 14

*Postscript to "The Background of Kummer's Proof"*, vol. 17

## Historical Transition

There is also an historical transition on which it would be agreeable to spend some time, but only if I had sufficient familiarity with the mathematical literature and correspondence of the of the period. Since I do not, I shall be brief.

If  $\alpha = \cos(2\pi/n) + i \sin(2\pi/n)$  the study of numbers

$$a + b\alpha + c\alpha^2 + \dots,$$

with  $a, b, c, \dots$  rational or integral is known as cyclotomy. As the name suggests and as we learned from Gauss, these numbers are the algebraic instruments for examining the division of the circle into  $n$  equal parts.

They have other uses, one of which, at least in certain cases, was discovered by Gauss, and was popular among young mathematicians of the succeeding generations, especially, Jacobi, Kummer, Eisenstein. The achievement of the young Gauss that mathematicians are inclined to emphasize is not the construction of the regular heptadecagon but the first complete, adequate proof of the law of quadratic reciprocity.

Consider the following sequence of numbers.

$$x^2 + 1, x = 1, 20$$

2, 5, 10, 17, 26, 37, 50, 65, 82, 101, 122, 145, 170, 197, 226, 257, 290, 325, 362, 401

Factored

2, 5,  $2 \cdot 5$ , 17,  $2 \cdot 13$ , 37,  $2 \cdot 5^2$ ,  $5 \cdot 1$ ,  $2 \cdot 41$ , 101,  $2 \cdot 61$ ,  $5 \cdot 29$ ,  $2 \cdot 5 \cdot 17$ , 197,  
 $2 \cdot 113$ , 257,  $2 \cdot 5 \cdot 29$ ,  $5^2 \cdot 13$ ,  $2 \cdot 181$ , 401.

With the exception of 2, all the primes that appear in these factorizations leave the remainder 1 upon division by 4.

# GEDÄCHTNISSREDE AUF GUSTAV PETER LEJEUNE DIRICHLET

VON

E. E. KUMMER.

[Gelesen in der öffentlichen Sitzung der Königl. Akademie der Wissenschaften  
am 5. Juli 1860.]

---

Es ist nicht zehn Jahre her, dass die drei Männer, denen unser deutsches Vaterland eine neue Blüthenperiode der mathematischen Wissenschaften verdankt, GAUSS, JACOBI und DIRICHLET noch lebten und noch thätig arbeiteten, den alten Ruhm tiefer Erkenntniss der abstractesten, sowie der concret in der Natur verwirklichten mathematischen Wahrheiten, welchen vor allen KEPLER und LEIBNITZ der deutschen Nation erworben hatten, glänzend zu erneuern und zu befestigen. Unsere Akademie hatte damals das Glück, zwei dieser hervorragenden Männer als active Mitglieder zu besitzen, JACOBI und DIRICHLET, welche persönlich befreundet, durch freie Mittheilung ihrer tiefen mathematischen Gedanken sich gegenseitig anregten und förderten, und auf die allgemeine Entwicklung der mathematischen Wissenschaften den nachhaltigsten Einfluss ausübten. JACOBI's frühzeitiger Tod war der erste unersetzliche Verlust, welcher die in unserem Vaterlande zur Blüthe entfaltete Wissenschaft traf. Die Bedeutung der Schöpfungen dieses mit seltenem Geiste begabten Forschers, die hervorragende Stellung, die er in der Geschichte der Mathematik für alle Zeiten einnehmen wird, hat DIRICHLET in der heut vor acht Jahren an dieser Stelle gehaltenen Gedächtnissrede so tiefeingehend und wahr geschildert, dass er dadurch dem Andenken des Dahingeschiedenen das schönste und würdigste Denkmal errichtet hat. Als vier Jahre nach JACOBI der greise GAUSS in dem unbestrittenen Ruhme des ersten Mathematikers seiner Zeit aus dem Leben schied, hatte dieser grosse allgemeine Verlust für unsere Akademie noch die beklagenswerthe Folge, dass DIRICHLET, als der einzige würdige Nachfolger des grossen Mannes, nach

Consider another sequence.

$$x^2 + 3, x = 1, 20$$

4, 7, 12, 19, 28, 39, 52, 67, 84, 103, 124, 147, 172, 199, 228, 259, 292, 327, 364, 403

Factored

$2^2$ , 7,  $2^2 \cdot 3$ , 19,  $2^2 \cdot 7 \cdot 3 \cdot 13$ ,  $2^2 \cdot 13$ , 67,  $2^2 \cdot 3 \cdot 7$ , 103,  $2^2 \cdot 31$ ,  $3 \cdot 7^2$ ,  $2^2 \cdot 43$ , 199,  
 $2^2 \cdot 3 \cdot 19$ ,  $7 \cdot 37$ ,  $262 \cdot 73$ ,  $3 \cdot 109$ ,  $2^2 \cdot 7 \cdot 13$ ,  $13 \cdot 31$ .

With the exception of 2 and 3 all the primes that appear as factors leave the remainder 1 upon division by 3.

Consider now the somewhat more mysterious sequence.

$$x^2 - 3, x = 1, 20$$

-2, 1, 6, 13, 22, 33, 46, 61, 78, 97, 118, 141, 166, 193, 222, 253, 286, 321, 358, 397

Factored

-  $1 \cdot 2$ ,  $1 \cdot 2 \cdot 3$ , 13,  $2 \cdot 11$ ,  $3 \cdot 11$ ,  $2 \cdot 23$ , 61,  $2 \cdot 3 \cdot 13$ , 97,  $2 \cdot 59$ ,  $3 \cdot 47$ ,  $2 \cdot 83$ ,  
 $193$ ,  $2 \cdot 3 \cdot 37$ ,  $11 \cdot 23$ ,  $2 \cdot 11 \cdot 13$ ,  $3 \cdot 107$ ,  $2 \cdot 179$ , 397

The primes here, those different from 2 and 3, leave both the remainders 1 and 3 upon division by 4 and the remainders 1 and 2 upon division by 3. So a rule is not at first apparent. One is quickly found. For example, 13 leaves the remainder 1 upon division by 4 and upon division by 3. On the other hand, 11 leaves the remainder 3 upon division by 4 and the remainder 2 upon division by 3. The same is true of 23, whereas 61 behaves like 13, as does 97. On examination of the other primes in the factorization, this appears to be a general rule.

These general rules appear for other expressions of the form  $x^2 \pm p$ , where  $p$  is a prime. They are called, for reasons that are not apparent and not so important, reciprocity laws. As one more example, consider  $p = 5$ .

$$x^2 - 5, x = 1, 20$$

-4, -1, 4, 11, 20, 31, 44, 59, 76, 95, 116, 139, 164, 191, 220, 251, 284, 319, 356, 395

Factored

-  $2^2$ , -1,  $2^2$ , 11,  $2^2 \cdot 5$ , 31,  $2^2 \cdot 11$ , 59,  $2^2 \cdot 19$ ,  $5 \cdot 19$ ,  $2^2 \cdot 29$ , 139,  $262 \cdot 41$ ,  
 191,  $262 \cdot 5 \cdot 11$ , 251,  $262 \cdot 71$ ,  $11 \cdot 29$ ,  $262 \cdot 89 \cdot 5 \cdot 79$ .

The primes that appear here, with the exception of 2 and 5, all leave the remainder 1 or the remainder 4 upon division by 5. They do not leave the remainder 2 or 3.

The quadratic reciprocity law was formulated in general during the latter part of the eighteenth century, above all by Adrien-Marie Legendre, and was proved at the very end of the century by the young Gauss.

There are also higher reciprocity laws, for  $x^m \pm p$ ,  $m = 3, 4, 5, \dots$ , but they cannot be expressed without cyclotomy. Even the quadratic reciprocity law is intimately related to cyclotomy as we shall have occasion to see. I confess that, as a student unaware of the history of the subject and unaware of the connection with cyclotomy, I did not find the law or its so-called elementary proofs appealing. I suppose, although I would not have – and could not have – expressed myself in this way that I saw it as little more than a mathematical curiosity, fit more for amateurs than for the attention of the serious mathematician that I then hoped to become. It was only in Hermann Weyl's book on the algebraic theory of numbers that I appreciated it as anything more. It is perhaps time for me to reread Weyl's book, a strange lumbering book, informed by an intellectual tension – conflict would be an inappropriate word – between two approaches to the theory, two approaches symbolized for Weyl by Kronecker and Dedekind, a tension that is still with us and, perhaps, still unresolved. Where, in the theory of numbers, do numbers end and geometry begin? The tension is, fortunately, not germane to Kummer although it does appear again, but not very obviously, in the aftermath of the recent proof of Fermat's theorem. There are some mathematicians who now place, in my view, too high hopes on the geometry. But these are arcane questions of interest to very few and their resolution will depend on results!

Although both Lagrange and Gauss were aware of possible applications of cyclotomy to Fermat's theorem, it was at first applied more to reciprocity laws. I add that reciprocity laws were every bit as important to Kummer as Fermat's theorem and were what first led him to take up cyclotomy. Reciprocity laws led to developments quite independent of Fermat that remain important to this day and that, indeed, were not of negligible import for the final resolution of the theorem.

Certainly the study of reciprocity laws entailed the study of factorization in the domains  $\mathbb{Z}(\alpha)$ , so that Jacobi, for example, had had some experience with it and was able to prevent Kummer from publishing at the very beginning of his study of cyclotomy some false conclusions.

“Der gute Junge” as he calls him in a letter to Dirichlet, with a certain condescension as he was only six years older, had without much ado assumed the decomposition of a prime  $p = \lambda n + 1$  in complexes of numbers formed from the  $\lambda$ -th roots of unity and deduced general theorems from this.

Si l'on faisait  $x = 0$  et  $\xi = 0$ , les quantités P et  $\Pi$  deviendraient

$$t^3 + Au^3 \quad \text{et} \quad \theta^3 + Av^3.$$

mais leur produit ne serait plus de la même forme, à cause que la quantité X ne deviendrait pas nulle.

Soit  $n = 4$ , en sorte que

$$p = t + ua \sqrt[4]{A} + xa^2 \sqrt[4]{A^2} + ya^3 \sqrt[4]{A^3} \quad \text{et} \quad a^4 - 1 = 0,$$

on trouvera

$$P = t^4 - A[2t^2(x^2 + uy) - 4tu^2x + u^4] + A^2(4txy^2 + x^4 - 4ux^2y + 2u^2y^2) - A^3y^4,$$

et le produit d'autant de fonctions de cette forme qu'on voudra sera toujours une fonction de la même forme, et ainsi de suite.

#### IV.

Si l'on avait à résoudre l'équation

$$r^n - As^n = q^n,$$

il est évident qu'on y parviendrait si l'on pouvait rendre chaque facteur de  $r^n - As^n$ , comme  $r - as \sqrt[n]{A}$ , égal à une puissance  $m^{\text{ième}}$ ,  $a$  étant toujours une des racines de l'équation  $a^n - 1 = 0$ .

Soit donc en général

$$r - sa \sqrt[n]{A} = p^n,$$

en sorte que

$$p = \sqrt[m]{r - sa \sqrt[n]{A}},$$

il est facile de concevoir que la valeur de  $p$  ne peut être exprimée que de cette manière

$$p = t + ua \sqrt[n]{A} + xa^2 \sqrt[n]{A^2} + ya^3 \sqrt[n]{A^3} + \dots + za^{n-1} \sqrt[n]{A^{n-1}};$$

cette quantité étant élevée à la puissance  $m$ , on aura (numéro précédent)

$$p^m = T + Va \sqrt[n]{A} + Xa^2 \sqrt[n]{A^2} + Ya^3 \sqrt[n]{A^3} + \dots + Za^{n-1} \sqrt[n]{A^{n-1}};$$

Mais, comme nous ne nous proposons pas ici de traiter cette matière à fond, nous ne nous y arrêterons pas davantage quant à présent: nous observerons seulement que M. de Fermat prétend, dans ses *Remarques sur Diophante*, avoir démontré en général ce théorème, que l'équation

$$r^n + s^n = q^n$$

n'est jamais résoluble d'une manière rationnelle lorsque  $n$  surpasse 2: mais ce Savant ne nous a pas laissé sa démonstration, et il ne paraît pas que personne l'ait encore trouvée jusqu'à présent. M. Euler a, à la vérité, démontré ce théorème dans le cas de  $n = 3$  et de  $n = 4$ , par une analyse particulière et très-ingénieuse, mais qui ne paraît pas applicable en général à tous les autres cas; ainsi, ce théorème est un de ceux qui restent encore à démontrer, et qui méritent le plus l'attention des Géomètres.



était restée propre aux entiers rationnels jusqu'au milieu du XVIII<sup>e</sup> siècle. C'est Euler qui, en 1770, ouvre un nouveau chapitre de l'Arithmétique en étendant, non sans témérité, la notion de divisibilité aux entiers d'une extension quadratique : cherchant à déterminer les diviseurs d'un nombre de la forme  $x^2 + cy^2$  ( $x, y, c$  entiers rationnels), il pose  $x + y\sqrt{-c} = (p + q\sqrt{-c})(r + s\sqrt{-c})$  ( $p, q, r, s$  entiers rationnels) et en prenant les normes des deux membres, il n'hésite pas à affirmer qu'il obtient ainsi tous les diviseurs de  $x^2 + cy^2$  sous la forme  $p^2 + cq^2$  ([81 a], (1), t. I, p. 422). En d'autres termes, Euler raisonne comme si l'anneau  $\mathbf{Z}[\sqrt{-c}]$  était principal ; un peu plus loin, il utilise un raisonnement analogue pour appliquer la méthode de « descente infinie » à l'équation  $x^3 + y^3 = z^3$  (il se ramène à écrire que  $p^2 + 3q^2$  est un cube, ce qu'il fait en posant  $p + q\sqrt{-3} = (r + s\sqrt{-3})^3$ ). Mais dès 1773, Lagrange démontre ([140], t. III, p. 695-795) que les diviseurs des nombres de la forme  $x^2 + cy^2$  ne sont pas toujours de cette forme, premier exemple de la difficulté fondamentale qui allait se présenter avec bien plus de netteté dans les études, poursuivies par Gauss et ses successeurs, sur la divisibilité dans les corps de racines de l'unité \* ; il n'est pas possible, en général, d'étendre directement à ces corps les propriétés essentielles de la divisibilité des entiers rationnels, existence du p.g.c.d. et unicité de la décomposition en facteurs premiers. Ce n'est pas ici le lieu de décrire en détail comment Kummer pour les corps de racines de l'unité [138] \*\*, puis Dedekind et Kronecker pour les corps de nombres algébriques quelconques, parvinrent à surmonter ce formidable obstacle par la création de la théorie des idéaux, un des progrès les plus décisifs de l'algèbre moderne. Mais Dedekind,

\* Gauss semble avoir un moment espéré que l'anneau des entiers dans le corps des racines  $n$ -èmes de l'unité soit un anneau principal ; dans un manuscrit non publié de son vivant ([95 a], t. II, p. 387-397), on le voit démontrer l'existence d'un processus de division euclidienne dans le corps des racines cubiques de l'unité, et donner quelques indications sur un processus analogue dans le corps des racines 5-èmes ; il utilise ces résultats pour démontrer par un raisonnement de « descente infinie » plus correct que celui d'Euler l'impossibilité de l'équation  $x^3 + y^3 = z^3$  dans le corps des racines cubiques de l'unité, signale qu'on peut étendre la méthode à l'équation  $x^5 + y^5 = z^5$ , mais s'arrête à l'équation  $x^7 + y^7 = z^7$  en constatant qu'il est impossible alors de rejeter *a priori* le cas où  $x, y, z$  ne sont pas divisibles par 7.

\*\* Dès son premier travail sur les « nombres idéaux », Kummer signale explicitement la possibilité d'appliquer sa méthode, non seulement aux corps de racines de l'unité, mais aussi aux corps quadratiques, et de retrouver ainsi les résultats de Gauss sur les formes quadratiques binaires ([138], p. 324-325).